

### **REMARKS**

Claims 1-22 are currently pending in the subject application and are presently under consideration. Claims 1, 12, 13, 16, 19, 21, 22 have been amended as shown at pages 3-6 of the Reply. Claims 11, 14, 18, and 20 have been cancelled. In addition, the specification has been amended as indicated at page 2

Applicants' representative thanks the Examiners for the courtesies extended during the telephonic interviews conducted on March 15, 2007. Examiners were contacted to discuss the objection to claims 11, 14, and 18 under 37 CFR 1.75(c), clarification of the notice regarding claim 22, and interpretation of the cited prior art reference with respect to claims 5, 6, 12, 13, 15 and 19. In particular, the prior art was discussed with respect to employing failure or timeouts during authentication in order to determine the encryption type being employed. Examiners believed that the claims were not clear with respect to this feature and that Fascenda may read on this aspect of the claimed invention. Examiners indicated that further consideration would be required upon receiving amended claims that are more clearly descriptive of this feature. Clarification was provided that claim 22 was not being rejected under 35 U.S.C. §112.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

#### **I. Objection of Claims 11, 14 and 18 Under 37 CFR 1.75(c)**

Claims 11, 14 and 18 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Claims 11, 14, and 18 have been cancelled. Therefore, this objection should be withdrawn.

#### **II. Objection of Claims 12, 13, 16 and 17**

Claims 12, 13, 16 and 17 are objected to because of the following informalities: the examiner notes the use of acronyms (Wi-fi, EAPOL) throughout the claims without first including a description in plain text, as required. Claims 9, 13, and 16 have been amended to address this objection. As such, this objection should be withdrawn.

### **III. Rejection of Claims 1-6, 8, 9, 11, 12, 21 and 22 Under 35 U.S.C. §102(e)**

Claims 1-6, 8, 9, 11, 12, 21 and 22 stand rejected under 35 U.S.C. §102(e) as being anticipated by Tsui (US 2005/0063338). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Tsui does not teach each and every element of the subject invention as recited in the subject claims.

A single prior art reference anticipates a patent claim only if it expressly or inherently describes each and every limitation set forth in the patent claim. *Trintec Industries, Inc., v. Top-U.S.A. Corp.*, 295 F.3d 1292, 63 U.S.P.Q.2D 1597 (Fed. Cir. 2002); *See Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ 2d 1051, 1053 (Fed. Cir. 1987). The identical invention must be shown in as complete detail as is contained in the ... claim. *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

The subject claims relates to identification of the type of security employed on a wireless network by detecting failures and timeouts during authentication. By recognizing failures or timeouts during particular portions of the authentication process, an iterative approach can narrow down the possible encryption types until identification is achieved. In particular, independent claim 1 (and similarly independent claims 12, 21, and 22) recites *a detection component that automatically identifies an encryption type of an available wireless network, wherein identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence.*

Tsui does not teach or suggest the aforementioned novel features as recited in the subject claims. The cited reference discloses a system for switching between available wireless networks when roaming. The system employs beacon information from the network to identify the network type. A code is downloaded from the beacon indicating the network protocol. The cited reference relies upon the beacon providing the network identifying information. Furthermore, the cited reference fails to discuss encryption types being employed on a wireless network. Tsui fails to disclose recognition of failures or timeouts during authentication in order to determine the encryption type being employed in the network. Therefore, Tsui fails to teach or suggest a detection component that identifies an encryption type of an available wireless

network, wherein identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence.

In view of the foregoing, applicants' representative respectfully submits that Tsui fails to teach or suggest all limitations of independent claims 1, 12, and 21 (and claims 2-6, 8, 9, and 11 that depend there from), and thus fails to anticipate the subject claims. Accordingly, withdrawal of this rejection is respectfully requested.

#### **IV. Rejection of Claims 4-10, 12, 14, 19 and 20 Under 35 U.S.C. §102(e)**

Claims 4-10, 12, 14, 19 and 20 stand rejected under 35 U.S.C. §102(e) as being anticipated by Fascenda (US 2004/0068653). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Tsui does not teach each and every element of the subject invention as recited in the subject claims.

Claim 20 has been cancelled. Independent claim 1 (and similarly independent claims 12 and 19) recites *a detection component that automatically identifies an encryption type of an available wireless network, wherein identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence*. Fascenda does not teach or suggest the aforementioned novel features as recited in the subject claims. The cited reference discloses a system employing access keys to authenticate users to a network. In particular, access keys are stored on a client machine for each network that the client machine will make a connection. The reference discloses that the access key along with accompanying network information is populated by an administrator or user in advance of connecting to a network. In order to identify a network, the BSSID of the network access point is employed. The BSSID is matched up with the appropriate access key and network information stored on the client machine. Fascenda relies upon the unique BSSID and stored pre-populated access key information to accomplish identification of the encryption type of the network. Fascenda, like Tsui, is silent regarding recognition of failures or timeouts during authentication in order to determine the encryption type being employed in the network. During the telephonic interview paragraph [0061] of Fascenda was mentioned as possibly anticipating this novel feature. However, this section of Fascenda merely discloses that if the user attempts to connect to a network and the access key does not match, the

access key may be associated with another network. The administrator would then have to manually populate any network type information associated with access key. Therefore, Fascenda fails to teach or suggest a detection component that identifies an encryption type of an available wireless network, wherein identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence.

In view of the foregoing, applicants' representative respectfully submits that Fascenda fails to teach or suggest all limitations of independent claims 1, 12, and 19 (and claims 4-10 and 14 that depend there from), and thus fails to anticipate the subject claims. Accordingly, withdrawal of this rejection is respectfully requested.

**V. Rejection of Claims 13, 15-18 and 20 Under 35 U.S.C. §103(a)**

Claims 13, 15-18 and 20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Fascenda (US 2004/0068653). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Fascenda does not teach each and every element of applicants' invention as recited in the subject claims.

To reject claims in an application under §103, an examiner must establish a *prima facie* case of obviousness. A *prima facie* case of obviousness is established by a showing of three basic criteria. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. See MPEP §706.02(j). The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. See *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Claim 20 has been cancelled. Claim 13 depends from independent claim 12. As discussed above, Fascenda fails to teach or suggest all limitations of independent claim 12. Moreover, independent claim 15 recites *determining whether a wireless network supports*

*802.1x; identifying the wireless network as an wired equivalent privacy network requiring a wired equivalent privacy key, if the wireless network does not support 802.1x. determining whether the wireless network supports wireless provisioning services, if the wireless network supports 802.1x; and, identifying the wireless network as an 802.1x network, if the wireless network does not supporting wireless provisioning services; and, identifying the wireless network as a wireless provisioning services supporting network, if the wireless network supports wireless provisioning services.* The subject claim discloses an iterative approach wherein failure of identification of one type of network is indicative of another network type. As conceded in the Office Action, Fascenda does not disclose the novel features of this claim. However, contrary to assertions in the Office Action, the novel features recited in claim 15 would not have been obvious to those skilled in the art. As discussed above, Fascenda relies on a BSSID and user populated network identification information associated with the BSSID for identification of network type. Fascenda fails to disclose an iterative approach as recited in the subject claim for identification of the network and encryption type. Accordingly, applicants' representative requests that the Examiner cite a specific prior art reference in support of her position pursuant to MPEP 2144.03 if the obviousness rejection in light of what was known to those skilled in the art at the time is maintained.

In view of the foregoing, applicants' representative respectfully submits that Fascenda fail to teach or suggest all limitations of independent claims 12 and 15 (and claims 13 and 16-19 that depend there from), and thus fails to make obvious the subject claimed invention. Accordingly, this rejection should be withdrawn.

**CONCLUSION**

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP552US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROC & CALVIN, LLP

/Himanshu S. Amin/

Himanshu S. Amin

Reg. No. 40,894

AMIN, TUROC & CALVIN, LLP  
24<sup>TH</sup> Floor, National City Center  
1900 E. 9<sup>TH</sup> Street  
Cleveland, Ohio 44114  
Telephone (216) 696-8730  
Facsimile (216) 696-8731